

Singapore Management University Institutional Knowledge at Singapore Management University

Research Collection School Of Information Systems

School of Information Systems

11-2016

A provably secure aggregate signature scheme for healthcare wireless sensor networks

Limin SHEN
Xidian University


Jianfeng MA
Xidian University

Ximeng LIU
Singapore Management University, xmliu@smu.edu.sg

Meixia MIAO
Xidian University

DOI: <https://doi.org/10.1007/s10916-016-0613-3>

Follow this and additional works at: https://ink.library.smu.edu.sg/sis_research

 Part of the [Information Security Commons](#), and the [Medicine and Health Sciences Commons](#)


Citation

SHEN, Limin; MA, Jianfeng; LIU, Ximeng; and MIAO, Meixia. A provably secure aggregate signature scheme for healthcare wireless sensor networks. (2016). *Journal of Medical Systems*. 40, (11), 1-10. Research Collection School Of Information Systems.

Available at: https://ink.library.smu.edu.sg/sis_research/3273

This Journal Article is brought to you for free and open access by the School of Information Systems at Institutional Knowledge at Singapore Management University. It has been accepted for inclusion in Research Collection School Of Information Systems by an authorized administrator of Institutional Knowledge at Singapore Management University. For more information, please email libIR@smu.edu.sg.

A Provably Secure Aggregate Signature Scheme for Healthcare Wireless Sensor Networks

Limin Shen^{1,2}  · Jianfeng Ma¹ · Ximeng Liu³ · Meixia Miao¹

Abstract Wireless sensor networks (WSNs) are being used in a wide range of applications for healthcare monitoring, like heart rate monitors and blood pressure monitors, which can minimize the need for healthcare professionals. In medical system, sensors on or in patients produce medical data which can be easily compromised by a vast of attacks. Although signature schemes can protect data authenticity and data integrity, when the number of users involved in the medical system becomes huge, the bandwidth and storage cost will rise sharply so that existing signature schemes are inapplicability for WSNs. In this paper, we propose an efficient aggregate signature scheme for healthcare WSNs according to an improved security model, which can combine multiple signatures into a single aggregate signature. The length of such an aggregate signature may be as long as that of an individual one, which can greatly decrease the bandwidth and storage cost for networks.

Keywords Wireless sensor networks · Healthcare wireless sensor networks · Medical system · Aggregate signature · Unforgeability · Coalition attack · Designated verifier

This article is part of the Topical Collection on *Patient Facing Systems*

Limin Shen
shenlimin@njnu.edu.cn

¹ School of Computer Science and Technology,
Xidian University, Xi'an, China

² School of Computer Science and Technology,
Nanjing Normal University, Nanjing, China

³ School of Information Systems, Singapore Management
University, Singapore, Singapore

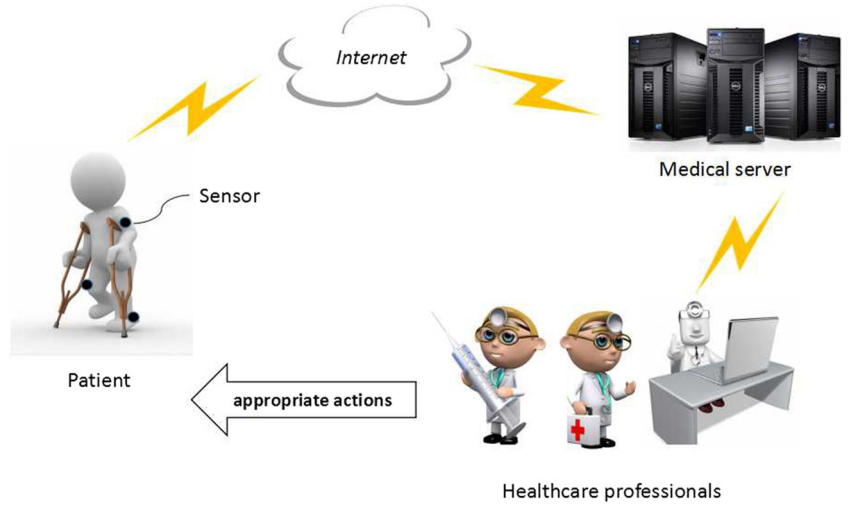
Introduction

Wireless sensor networks (WSNs) contain massive small, cheap and resource-constrained sensors which can monitor the physical world from remote locations [1]. Due to these characteristics, two types of healthcare WSNs (HWSNs), called implanted and wearable, have been paid much attention in e-healthcare area [2–4]. In implanted application, the user's body is inserted by implantable medical devices, such as endoscope capsule, cardiac arrhythmia monitors, etc. In wearable application, sensors are put on the patient's body or at immediate proximity to patients dressed in wearable devices for blood pressure monitoring, temperature measurement, pH monitoring, respiration monitoring, and so on. Therefore the patients are not subject to regional restrictions. In both the above applications, patients with the wearable HWSNs can walk around freely and get the proper medical observation. The service process is shown in Fig. 1. The data generated by these sensors are transmitted to the medical server, which can process the data and provide the information to the healthcare professionals for further analysis and appropriate actions to patients [5, 6].

Despite such advantages in HWSNs, medical data can be easily compromised by a vast of attacks, such as data interception and data tampering, etc. Although signature schemes can protect data authenticity and data integrity, when the medical system become large scale, the existing signature schemes are inapplicability for HWSNs. Moreover, sensors always suffer from the limited storage and processing resources. Therefore, designing a secure and efficient data aggregation method is very significant for HWSNs.

The concept of *general aggregate signatures* was introduced by Boneh et al. [7]. In a general aggregate signature

Fig. 1 Service Process



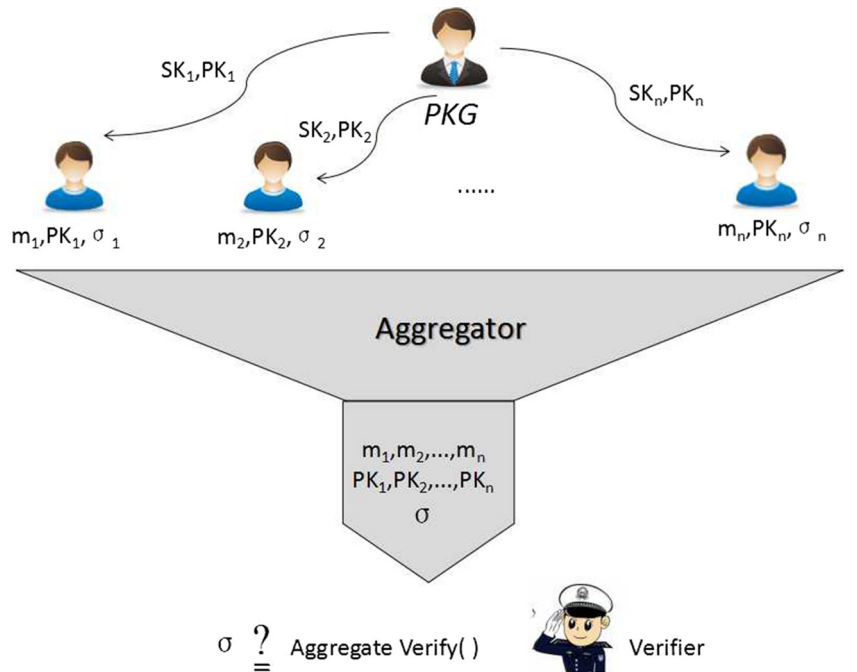
scheme (Fig. 2), anyone can aggregate many signatures on different messages from multiple users into a single short one. The length of such an aggregate signature can be as long as that of an individual one, so it can reduce the bandwidth and storage cost for networks.

Our Contributions

In order to solve the problem of limited resources and integrity of WSNs, an efficient aggregate signature scheme for HWSNs is presented. The main contributions are summarized as follows:

- We re-examine the security model for aggregate signature schemes defined in [7] and point out it does not fully address the threat of coalition attacks [8, 9]. To address this issue, we suggest to modify the security model for aggregate signature schemes. The shining point of our new security model is that the unique way for generating a valid aggregate signature is to use all valid individual signatures. So we give the adversary the capability of launching any coalition attack. The adversary can successfully attack the scheme only if it outputs a valid aggregate signature using one set of individual signatures including some invalid ones.

Fig. 2 Schematic Diagram of the Aggregate Signature Scheme



- We present a system model of HWSNs which contain four components: authorized healthcare professionals, medical server, aggregator and a large number of sensors. The system model should solve three problems in HWSNs: network congestion, collusion attacks and data integrity protection.
- We give a new aggregate signature scheme for HWSNs based on the schemes [7, 10]. Our scheme not only keeps the basic signature scheme's good feature, but also resists coalition attacks. Furthermore, it can protect data authenticity and integrity.

Related Work

Boneh et al. [7] presented the concept of *general aggregate signatures*, in which anyone can combine multiple signatures from distinct users into a short aggregate signature, so the aggregator only needs to transmit the aggregate signature instead of all the single signatures. Due to the character of compression, aggregate signature technology is useful for lowering bandwidth and storage cost for transmitting many message-signature pairs. Hence, designing efficient and secure aggregate signature schemes has been a significant research field since the very beginning of its birth. Recently, a number of aggregate signature schemes have been presented [11–22]. Unfortunately, most of the former schemes can not resist coalition attacks [8, 9, 23].

Coalition attack means that some signers use a set of individual signatures which includes at least one invalid single signature to generate a valid aggregate signature. This attack is not clearly addressed in the former security models. If such an attack is successful, the resulted aggregate signature's validity will not guarantee the validity of all single signatures involved in the aggregation, which clearly breaches the aggregate signature scheme's security requirements. Hence, an appropriate security model for the aggregate signature scheme should take coalition attacks into consideration. Thus, for the construction of an aggregate signature scheme, besides the secure basic signature scheme, a secure *aggregate algorithm* resistant to coalition attacks is an imperative problem to be solved.

Organization

In the following section, we give the preliminaries demanded in this paper. “[Security Model and System Model](#)” presents our improved security model of the aggregate signature scheme and the system model of HWSNs. In “[A New Aggregate Signature Scheme](#)”, we give our aggregate signature scheme with a designated verifier for HWSNs, then provide the security analysis, performance

analysis and the typical applications. Finally, “[Conclusion](#)” is the conclusion.

Preliminaries

This section revisits the basic concepts which are prerequisite in this paper. We use some notations [10] in the following paper. Let \mathbb{G}_1 and \mathbb{G}_2 denote two multiplicative cyclic groups with the same prime order p ; let g_1 be a generator in \mathbb{G}_1 and g_2 be a generator in \mathbb{G}_2 . \mathbb{G}_T is an additional group such that $|\mathbb{G}_1| = |\mathbb{G}_2| = |\mathbb{G}_T|$. Finally, let a computable isomorphism $\psi : \mathbb{G}_2 \rightarrow \mathbb{G}_1$ with $\psi(g_2) = g_1$.

Bilinear Pairing

Let $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, p, g_1, g_2$ be the same as mentioned above. Let $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ be a bilinear pairing with the following properties:

- Bilinear: for all $h \in \mathbb{G}_1, k \in \mathbb{G}_2, \mu, \nu \in \mathbb{Z}_p^*$, $\hat{e}(h^\mu, k^\nu) = \hat{e}(h, k)^{\mu\nu}$.
- Non-degenerate: $\hat{e}(g_1, g_2) \neq 1_T$, where 1_T is the identity element of \mathbb{G}_T .
- Computable: for all $h \in \mathbb{G}_1, k \in \mathbb{G}_2$, $\hat{e}(h, k)$ is efficiently computable.

Complexity Assumptions

In this section, we give some complexity assumptions [7, 10] needed in the following paper.

Computational Diffie-Hellman (CDH) Problem Given the elements $g, g^\mu, g^\nu \in \mathbb{G}$, to compute $g^{\mu\nu} \in \mathbb{G}$. The CDH assumption states that the CDH problem is hard. Let \mathcal{A} be a CDH problem solver, and let $Adv_{\mathcal{A}}^{CDH}$ be the advantage of \mathcal{A} in solving the CDH problem, then

$$Adv_{\mathcal{A}}^{CDH} = Pr[\mathcal{A}(g, g^\mu, g^\nu) = g^{\mu\nu} : \mu, \nu \in \mathbb{Z}_p^*]. \quad (1)$$

Decision Diffie-Hellman (DDH) Problem Given the elements $g, g^\mu, g^\nu, g^\kappa \in \mathbb{G}$, output Y if $\kappa = \mu\nu$, output N otherwise.

Computational Co-Diffie-Hellman (co-CDH) Problem Given the elements $h \in \mathbb{G}_1$ and $g_2, g_2^\mu \in \mathbb{G}_2$, compute $h^\mu \in \mathbb{G}_1$.

Decision Co-Diffie-Hellman (co-DDH) Problem Given the elements $h, h^\nu \in \mathbb{G}_1$ and $g_2, g_2^\mu \in \mathbb{G}_2$, output Y if

$\mu = v$, output N else. We say that the tuple (g_2, g_2^μ, h, h^μ) is a co-Diffie-Hellman tuple if the answer is Y .

Note that when $\mathbb{G}_1 = \mathbb{G}_2$ and $g_1 = g_2$, the co-CDH problem reduces to CDH problem, and co-DDH problem reduces to DDH problems.

Co-Gap Diffie-Hellman (co-GDH) Group Pair If co-DDH is easy but co-CDH is hard in $(\mathbb{G}_1, \mathbb{G}_2)$, then we define the pair of groups $(\mathbb{G}_1, \mathbb{G}_2)$ be a Co-GDH group pair. Please refer to [7, 10] for the detailed definition.

Outline of Aggregate Signature Schemes

Definition of Aggregate Signature Schemes

Figure 2 is the schematic diagram of an aggregate signature scheme. A general aggregate signature scheme comprises of a basic signature scheme, an aggregate algorithm and an aggregate verify algorithm. More specifically, a general aggregate signature scheme comprises six algorithms: Setup, Key Extract, Sign, Verify, Aggregate and Aggregate Verify. Please refer to [7] for more detailed description.

Revisiting The Security Model in [7]

As presented in [7], the motivation of aggregate signatures is to create one aggregate signature from many single signatures which are generated by individual users. This aggregate signature has the property that it can convince the verifier that each user actually signed its message, respectively. This indicates that inputting all the valid individual signatures into the *aggregate algorithm* is the only way to generate a valid aggregate signature.

The adversary \mathcal{A} is only dispensed a single public key in the security model [7], its target is to existentially forge an aggregate signature. \mathcal{A} 's power is that \mathcal{A} can choose all public keys except the challenge one, can access to a sign oracle on the challenge key. Then, the advantage of \mathcal{A} , $Adv_{AggSig_{\mathcal{A}}}$, is defined to be the success probability in the following game.

Setup The aggregate forger \mathcal{A} is given a public key PK_1 , which is randomly generated.

Queries Proceeding adaptively, \mathcal{A} requests signatures with PK_1 on messages of his choice.

Response Lastly, \mathcal{A} outputs $r - 1$ added public keys PK_2, \dots, PK_r . Here $r \leq N$, N is the game parameter. \mathcal{A} also outputs *distinct* messages $\{M_1, \dots, M_r\}$. Then in the end, \mathcal{A} outputs an aggregate signature σ of the r users under the public keys $\{PK_1, \dots, PK_r\}$ on corresponding messages $\{M_1, \dots, M_r\}$.

The forger \mathcal{A} wins the game if the following conditions are satisfied:

- σ is a valid aggregate under public keys $\{PK_1, \dots, PK_r\}$ on messages $\{M_1, \dots, M_r\}$;
- Signature on (M_1, PK_1) has been not queried by \mathcal{A} .

Obviously, in the above security model, the adversary \mathcal{A} can successfully forge a valid aggregate signature if \mathcal{A} can forge the single signature, that is to say, \mathcal{A} just needs to attack the security of the basic signature scheme involved. So, it is easy to suffer from coalition attacks. If someone can successfully implement such attacks, that is to say, an aggregate signature is not able to convince the verifier that each signer really signed the initial message.

Security Model and System Model

Improved Security Model of the Aggregate Signature Scheme

Clearly, a existentially unforgeable aggregate signature scheme requires both the involved basic signature scheme and the *aggregate algorithm* should be existentially unforgeable. However, the adversary merely forge the single signature in most of the former security model, i.e. they only attack the security of the involved basic signature scheme. Therefore, we mainly consider the *aggregate algorithm*'s security in the following improved security model.

The capacity of an adversary in the former security model for aggregate signature is limited, because the adversary can not access all the secret signing keys. We make some modification to the security model defined in [7]. In our improved security model, we permit the adversary to get all signers' secret signing keys by accessing the relevant oracles. The adversary's purpose is to forge a valid aggregate signature using a set of individual signatures which contains at least one invalid individual signature. Now we give our improved security model of the aggregate signature scheme through the coming game between an adversary \mathcal{A} and a challenger \mathcal{C} . The game is shown in Fig. 3.

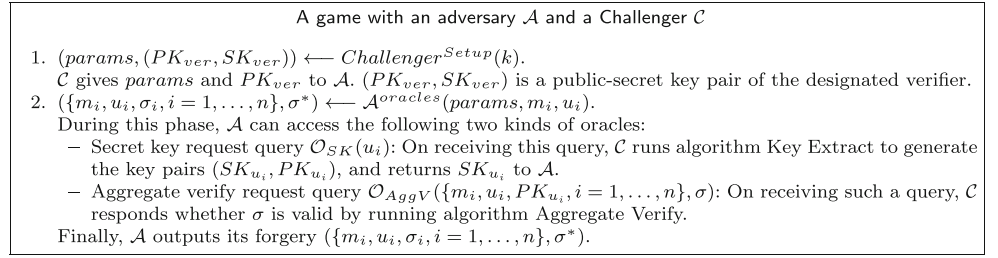
\mathcal{A} wins the game if the following conditions are satisfied:

- σ^* is a valid aggregate signature under public keys PK_{u_i} and messages $m_i, i = 1, \dots, n$.
- At least one single signature used to generate σ^* is invalid.

We denote $Adv_{AggSig_{\mathcal{A}}}$ be the adversary's advantage in attacking an aggregate signature scheme as its success probability in winning the above game.

Definition We say an aggregate signature scheme is (t, n) -secure against an adversary \mathcal{A} , if \mathcal{A} runs in polynomial time

Fig. 3 Game



t , the forged aggregate signature is by at most n users, and Adv_{AggSig_A} is negligible.

System Model

In HWSNs, integrity, authenticity, confidentiality are considered as three significant aspects [2, 24]. It is crucial that no data falsify during transmissions. The main consideration of our system model is to protect data authenticity and integrity while reducing bandwidth and storage cost for HWSNs. Our system model for HWSNs consists of four parts as shown in Fig.4: authorized healthcare professionals, medical server, aggregator and a large number of sensors.

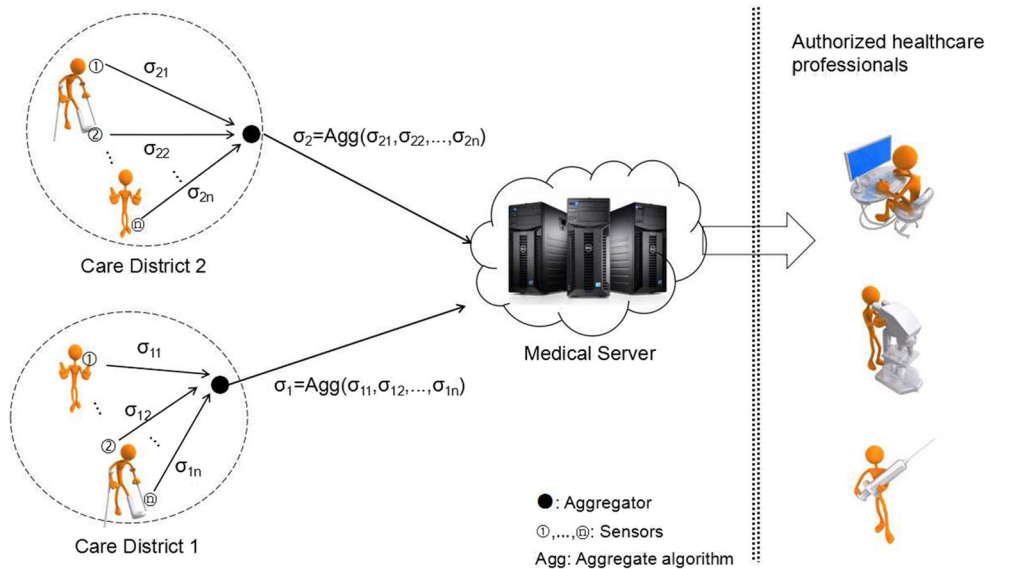
- **Authorized healthcare professionals** have a certain ability to calculation and communication, can analyze the data generated by the sensors, and can make appropriate actions for patients.
- **Medical server** has a strong computing power and storage space, can process all original big data collected by sensors, can provide the patients' data information to healthcare professionals. At the beginning, every medical server, will receive its public-secret key pair $(PK_{server}, SK_{server})$, and publish the public key

PK_{server} . In our system, medical server also works as the designated verifier who can verify the aggregate signatures using its secret key SK_{server} .

- **Aggregator** has a certain ability to calculation and communication, can get the medical server's public key PK_{server} , can produce the aggregate signature and send it to the medical server. Every care district consists of one aggregator and many sensors.
- **Sensors** are resource-limited devices, each sensor belongs to one care district. We assume that when sensor i is deployed, it is embedded with its public-secret key pair $(PK_i, SK_i) = (X_i, x_i)$. Each sensor i is able to sign messages generated from the physical world using its private key x_i , and send messages and its signatures to their aggregator.

For health monitoring in the system model, sensors are placed on or in a patient's body. These sensors can sense the patient's blood pressure, pH-value and heart rate, and can transmit these information to medical server via the aggregator. However, data can be easily compromised by various attacks during the transmission and aggregation, such as data tampering, coalition attacks. Thus, three critical problems should be considered in our system:

Fig. 4 HWSNs System Model



- How can medical data integrity in HWSNs be protected?
- How can storage cost and bandwidth be reduced?
- How can coalition attacks in HWSNs be resisted?

In order to guarantee authenticity and integrity of medical data, each sensor creates signatures using its private key for the information generated by itself. Then the sensors in the same care district send the signatures to their aggregator. For example, in Fig. 4, in Care District 1, every sensor i generates message m_i and the corresponding signatures σ_{1i} , sends them to the aggregator ($i = 1, 2, \dots, n$). Then the aggregator will send these information to the medical server. In order to avoid network congestion, the aggregator should adopt data aggregation methods. In our system, the aggregator generates an aggregate signature $\sigma_1 = \text{Agg}(\sigma_{11}, \sigma_{12}, \dots, \sigma_{1n})$ using the aggregate signature technique, and sends σ_1 to the medical server, then the medical server verifies σ_1 . If σ_1 is valid, the medical server provides the patients' data information to healthcare professionals, which make suitable actions to patients. Else if σ_1 is invalid, the medical server rejects it. Figure 5 illustrates the scheme flow of HWSNs.

The aggregate signature technique can compress signatures, instead of transmitting many message-signature pairs. In the following section, we give an efficient aggregate signature scheme for HWSNs. To overcome coalition attacks, each aggregator adopts the designated verifier's public key PK_{server} and a collision resistant hash function H to generate the aggregate signature. In our system, the designated verifier is just the medical server.

A New Aggregate Signature Scheme

Construction

In this section, we provide a secure aggregate signature scheme. We adopt the famous BLS short signature scheme in [10] as the basis to construct our scheme. Our scheme can guarantee that if the involved basic signature scheme is existentially unforgeable, then all signers involved in the aggregate algorithm really signed the corresponding message once the aggregate signature is valid. The new scheme consists of six algorithms: Setup, Key Extract, Sign, Verify, Aggregate and Aggregate Verify.

Setup Let $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, p, \hat{e}, g_1, g_2$ and ψ be the same as ones defined in “Preliminaries”. H, H_1 are full-domain collision resistant hash functions. $H : \{0, 1\}^* \rightarrow \mathbb{G}_1, H_1 : \{0, 1\}^* \rightarrow \mathbb{Z}_p^*$. Let $(PK_{server}, SK_{server})$ be a random

public-secret verification key pair of the medical server, where $SK_{server} = s \in_R \mathbb{Z}_p^*, PK_{server} = g_2^s$.

Key Extract For a specific sensor, pick $x \in \mathbb{Z}_p^*$ randomly, then compute $X = g_2^x \in \mathbb{G}_2$. The sensor's public-secret key pair is $(PK, SK) = (X, x)$.

Sign For a specific sensor, given a message $m \in \{0, 1\}^*$ and secret key x , compute the signature σ_s as the following: $h = H(m), \sigma_s = h^x$.

Verify Given a signature σ_s , a message m and a specific sensor's public key X , compute $h = H(m)$, and then check if the equation

$$\hat{e}(\sigma_s, g_2) = \hat{e}(h, X) \quad (2)$$

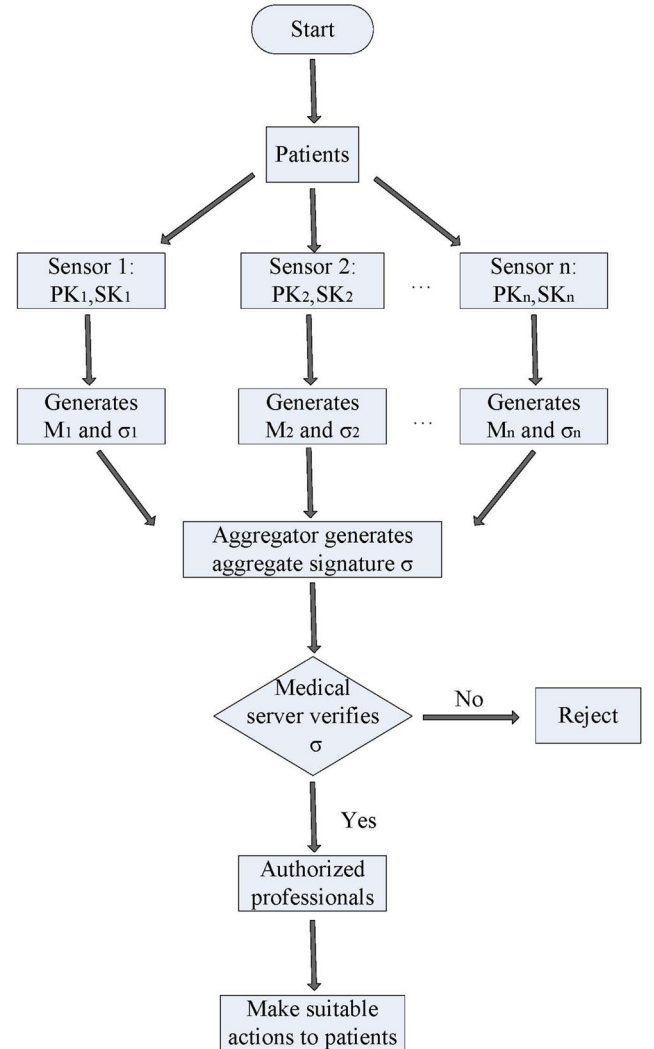


Fig. 5 HWSNs Flowchart

Table 1 Definition of notations

Notation	Definition
<i>aggregate</i>	aggregate scheme
<i>un-aggregate</i>	un-aggregate scheme
$ m $	the overall length of $\{m_1, m_2, \dots, m_n\}$
M	the computation cost of a scalar multiplication calculation in \mathbb{G}_1 or \mathbb{G}_2
$M_{\mathbb{G}_T}$	the computation cost of a multiplication calculation in \mathbb{G}_T
E	the computation cost of an exponentiation operation in \mathbb{G}_1 or \mathbb{G}_2
$E_{\mathbb{G}_T}$	the computation cost of an exponentiation operation in \mathbb{G}_T
P	the computation cost of a pairing operation in \mathbb{G}_T

holds or not. If it holds, then accept; otherwise, do not accept.

Aggregate Define $U \in \mathcal{U}$ as the aggregating subset of sensors, and define $n = |U|$. Each sensor $u_i \in U$ with public key X_i generates a signature σ_i on a message $m_i \in \{0, 1\}^*$ which sensed by itself ($i = 1, \dots, n$). Moreover, denote PK_{server} as the public key of the medical server (s is the corresponding secret key, i.e. $PK_{server} = g_2^s$). Compute

$$\tau = H_1(\hat{e}(\sigma_1, PK_{server}), \dots, \hat{e}(\sigma_n, PK_{server})), \quad (3)$$

$$\sigma' = \prod_{i=1}^n \sigma_i, \quad (4)$$

$$\sigma = \sigma'^\tau. \quad (5)$$

The aggregate signature is σ .

Aggregate Verify Given an aggregating signers subset U of n sensors $\{u_1, \dots, u_n\}$, and the public key $X_i \in \mathbb{G}_2$ for every sensor u_i ($i = 1, \dots, n$), an aggregate signature $\sigma \in \mathbb{G}_1$ on the initial messages $\{m_1, \dots, m_n\}$. To verify the aggregate signature σ , for every $i, 1 \leq i \leq n = |U|$, the medical server computes $h_i = H(m_i)$, and accepts if the following equation holds:

$$\hat{e}(\sigma, g_2) = \prod_{i=1}^n \hat{e}(h_i^{\tau'}, X_i), \quad (6)$$

where

$$\tau' = H_1(\hat{e}(h_1^s, X_1), \dots, \hat{e}(h_n^s, X_n)). \quad (7)$$

Security Analysis

The security proof of existential unforgeability on the basic signature scheme involved has been given carefully in Theorem 1 of [10], which assumes $(\mathbb{G}_1, \mathbb{G}_2)$ is a co-GDH group pair, and proves the EUF-CMA (existentially unforgeable against adaptive chosen message attacks) secure [25, 26] in the random oracle model. So we only prove the security of the above *aggregate algorithm*.

Theorem 1 Suppose the hash function H_1 is collision resistant. Then the aggregate signature in the above aggregate signature scheme is valid, if and only if each individual signature used in the aggregation is valid.

Proof If each individual signature involved in the aggregation is valid, then

$$\begin{aligned} \hat{e}(\sigma_i, g_2) &= \hat{e}(h_i, X_i), \hat{e}(\sigma_i, PK_{server}) \\ &= \hat{e}(\sigma_i, g_2^s) \\ &= \hat{e}(h_i^s, X_i), i = 1, \dots, n. \end{aligned}$$

So we have

$$\begin{aligned} \tau &= H_1(\hat{e}(\sigma_1, PK_{server}), \dots, \hat{e}(\sigma_n, PK_{server})) \\ &= H_1(\hat{e}(h_1^s, X_1), \dots, \hat{e}(h_n^s, X_n)) \\ &= \tau' \end{aligned}$$

and

$$\begin{aligned} \hat{e}(\sigma, g_2) &= \hat{e}((\prod_{i=1}^n \sigma_i)^{\tau'}, g_2) \\ &= \prod_{i=1}^n \hat{e}(\sigma_i^{\tau'}, g_2) \\ &= \prod_{i=1}^n \hat{e}(h_i^{\tau'}, X_i). \end{aligned}$$

That is to say, the resulting aggregate signature σ is valid.

In addition, if the aggregate signature σ is valid, then we have

$$\hat{e}(\sigma, g_2) = \prod_{i=1}^n \hat{e}(h_i^{\tau'}, X_i)$$

and

$$\begin{aligned} \tau' &= H_1(\hat{e}(h_1^s, X_1), \dots, \hat{e}(h_n^s, X_n)) \\ &= H_1(\hat{e}(\sigma_1, PK_{server}), \dots, \hat{e}(\sigma_n, PK_{server})) \\ &= \tau. \end{aligned}$$

Table 2 Performance comparison of communication cost

	Un-aggregate	Aggregate
Sensors \rightarrow Aggregator	$n \mathbb{G}_1 + m $	$n \mathbb{G}_1 + m $
Aggregator \rightarrow Medical Server	$n \mathbb{G}_1 + m $	$ \mathbb{G}_1 + m $

As H_1 is collision resistant, we have $\hat{e}(\sigma_i, PK_{server}) = \hat{e}(h_i^s, X_i)$, and hence $\hat{e}(\sigma_i, g_2) = \hat{e}(h_i, X_i)$, for each $i = 1, \dots, n$. This indicates each individual signature involved in the aggregation is valid. Equations (3, 4 and 5) ensure that the medical server can not forge the aggregate signature.

Therefore, with the security proof of schemes in [7, 10], we can get the conclusion that our aggregate signature scheme is existentially unforgeable. \square

Observation By now, most the known aggregate signature schemes are insecure against coalition attacks. Some of them can be modified to secure ones by using a collision resistant hash function and the verifier's public key in the aggregating process, which can ensure that an aggregate signature's validity implies each individual signature's validity involved in the aggregation. And from the above analysis, we are able to find that the coalition attacks are directed at the *aggregate algorithm*, so such attacks are appropriate not only to public key infrastructures but also to certificateless and identity-based surroundings.

Performance Analysis

In this section, we evaluate the performance of our scheme. We firstly retrospect each component's function in our scheme. Authorized healthcare professionals can analyze the data generated by the sensors and make appropriate actions for patients. Medical server has a strong computing power and storage space, can process all original big data collected by sensors. Aggregator can produce the aggregate signature and send it to the medical server. Sensors have limited resources, can collect the health information of patients and send the information to their aggregator. The description of some notations to be used in this section is given in Table 1.

Communication Cost

Table 2 gives the communication cost comparison of two versions: un-aggregate scheme and aggregate scheme.

The comparison indicates that the aggregate scheme can reduce $(n - 1)|G_1|$ transmission cost in one process of data aggregation, concurrently, can reduce $(n - 1)|G_1|$ storage cost. Therefore, our scheme is efficient in data aggregation method for HWSNs.

Efficiency Comparison

Table 3 gives the efficiency comparison of our aggregate scheme with some existing pairing based schemes. Our scheme can resist coalition attacks while more pairing operations are needed during the process of aggregate verify (recall that the medical server has a strong computing power to verify the aggregate signature).

Application

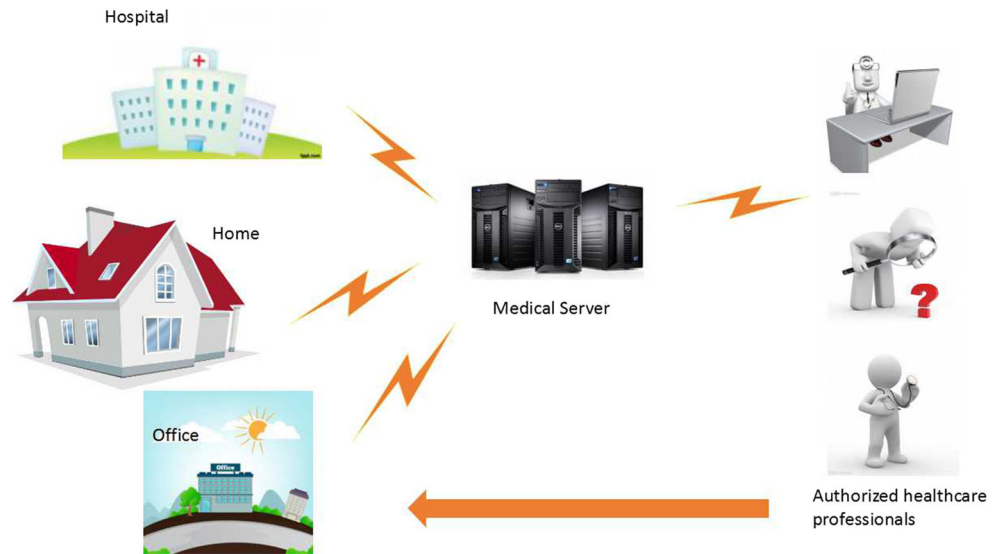
WSNs have been widely applied in many areas, such as biomedical health monitoring and target tracking. Our aggregate signature scheme for HWSNs not only can guarantee authenticity and integrity of medical data, but also can avoid network congestion. So it has practical applications in healthcare medical system, such as medical monitoring system and home monitoring network system, etc. The following is the typical applications and Fig. 6 illustrates the general process.

- HWSNs in hospitals make the healthcare professionals gain more accurate physiological parameters, then improve the life quality of patients, especially for age-related chronic disease. Sensors can continuously generate huge data on patient physiological signals, which will be beneficial to patient healthcare and for further research.
- In-home healthcare of elderly becomes an urgent social problem, the traditional healthcare system cannot satisfy the present developmental needs. Furthermore, some patients can be recovering at home (even in the office), and they also need the in-home healthcare. HWSNs can fix this, it can minimize the need for healthcare professionals. The elderly and patients with the wearable HWSNs can move freely at home. Sensors generate the real-time data and transmit these information to the medical server. Finally, healthcare

Table 3 Efficiency comparison of some pairing based aggregate schemes

Scheme	Sign	Aggregate verify	Coalition attacks resistance
[7]	E	$(n + 1)P + (n - 1)M_{G_T}$	No
[11]	M	$(n + 2)P + nM_{G_T}$	No
[13]	E	$(n + 1)P + (n - 1)M_{G_T}$	No
[17]	M	$(n + 1)P + (n - 1)M_{G_T} + nM$	No
Ours	E	$(2n + 1)P + 2nE_{G_T} + (n - 1)M_{G_T}$	Yes

Fig. 6 Typical Applications



professionals will get these data for further analysis and make appropriate actions to those who need further treatments.

Conclusion

In this paper, we modified the aggregate signature's security model defined in [7] combining with the coalition attacks [8, 9]. Then for healthcare WSNs, we proposed an aggregate signature scheme, which achieves not only data authenticity and integrity, but also the lower cost of storage and communication. Furthermore, our scheme not only keeps the Boneh et al. scheme's good feature about a short signature, but also resists coalition attacks of aggregate signature schemes. Next, we will focus on designing secure aggregate signature schemes without using the medical server's public key for HWSNs.

Acknowledgments This work is supported by National Natural Science Foundation of China (Grant No. U1405255, 61370078, 61672289, 61502237 and 61572198), National High Technology Research and Development Program (863 Program) of China (No. 2015AA016007). The authors would like to thank the anonymous reviewers and the editor for their constructive comments that have helped us to improve this paper.

References

1. Mahmoud, M., and Shen, X., A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks. *IEEE Trans. Parallel Distrib. Syst.* 23(10):1805–1818, 2012.
2. Wang, X., and Zhang, Z., Data Division Scheme Based on Homomorphic Encryption in WSNs for Health Care. *J. Med. Syst.* 39(12):1–7, 2015.
3. He, D. B., Zeadally, S., and Wu, L., Certificateless public auditing scheme for cloud-assisted wireless body area networks. *IEEE Syst. J.*, 2015. doi:[10.1109/JSYST.2015.2428620](https://doi.org/10.1109/JSYST.2015.2428620).
4. He, D. B., Zeadally, S., Kumar, N., and Lee, J. H., Anonymous authentication for wireless body area networks with provable security. *IEEE Syst. J.*, 2016. doi:[10.1109/JSYST.2016.2544805](https://doi.org/10.1109/JSYST.2016.2544805).
5. Egbogah, E., and Fapojuwo, A., A survey of system architecture requirements for health care-based wireless sensor networks. *Sensors* 11(3):4875–4898, 2011.
6. He, D. B., Kumar, N., Wang, H., Wang, L., Choo, K. K. R., and Vinel, A., A provably-secure cross-domain handshake scheme with symptoms-matching for mobile healthcare social network. *IEEE Trans. Dependable Secure Comput.*, 2016. doi:[10.1109/TDSC.2016.2596286](https://doi.org/10.1109/TDSC.2016.2596286).
7. Boneh, D., Gentry, C., Lynn, B., and Shacham, H., Aggregate and verifiably encrypted signatures from bilinear maps. In: *Proceedings of Eurocrypt 2003, Warsaw, Poland*. LNCS 2656: 416–432, 2003.
8. Zhang, F., Shen, L., and Wu, G., Notes on the security of certificateless aggregate signature schemes. *Inf. Sci.* 287:32–37, 2014.
9. Shen, L., Ma, J., Liu, X., Wei, F., and Miao, M., A secure and efficient id-based aggregate signature scheme for wireless sensor networks. *IEEE Internet of Things Journal*, 2016. doi:[10.1109/JIOT.2016.2557487](https://doi.org/10.1109/JIOT.2016.2557487).
10. Boneh, D., Lynn, B., and Shacham, H., Short signatures from the weil pairing. In: *Proceedings of Asiacrypt 01*, LNCS 2248: 514–532, 2001.
11. Shao, Z., Enhanced aggregate signatures from pairings. In: *Proceedings of CISC 2005, Springer-Verlag*, LNCS 3822: 140–149, 2005.
12. Gentry, G., and Ramzan, Z., Identity-based aggregate signatures. In: *Proceedings of Public Key Cryptography 2006*, LNCS 3958: 257–273, 2006.
13. Bellare, M., Namprempre, C., and Neven, G., Unrestricted aggregate signatures. In: *Proceedings of ICALP'2007, Springer-Verlag*, LNCS 4596: 411–422, 2007.
14. Zhang, L., and Zhang, F., A new certificateless aggregate signature scheme. *Comput. Commun.* 32(6):1079–1085, 2009.

15. Shim, K. A., An ID-based aggregate signature scheme with constant pairing computations. *J. Syst. Softw.* 83(10):1873–1880, 2010.
16. Zhang, L., Qin, B., Wu, Q., and Zhang, F., Efficient many-to-one authentication with certificateless aggregate signatures. *Comput. Netw.* 54(14):2482–2491, 2010.
17. Wen, Y., Ma, J., and Huang, H., An Aggregate Signature Scheme with Specified Verifier. *Chin. J. Electron.* 20(2):333–336, 2011.
18. Liu, X., Zhu, H., Ma, J., Li, Q., and Xiong, J., Efficient attribute based sequential aggregate signature for wireless sensor networks. *International Journal of Sensor Networks* 16(3):172–184, 2014.
19. Hohenberger, S., Koppula, V., and Waters, B., Universal Signature Aggregators. In: *Proceedings of EUROCRYPT 2015*. Springer Berlin Heidelberg, LNCS 9057: 3–34, 2015.
20. Hartung, G., Kaidel, B., Koch, A., and et al., Fault-Tolerant Aggregate Signatures. In: *Proceedings of Public Key Cryptography-PKC 2016*, Springer Berlin Heidelberg, LNCS 9614: 331–356, 2016.
21. Zhang, L., Hu, C., Wu, Q., Domingoferrer, J., and Qin, B., Privacy-preserving vehicular communication authentication with hierarchical aggregation and fast response. *IEEE Trans. Comput.* 65(8):2562–2574, 2016.
22. Zhang, L., Wu, Q., Domingo-Ferrer, J., Qin, B., and Hu, C., Distributed Aggregate Privacy-Preserving Authentication in VANETs. *IEEE Trans. Intell. Transp. Syst.*, 2016. doi:[10.1109/TITS.2016.2579162](https://doi.org/10.1109/TITS.2016.2579162).
23. Viet, N. Q., and Ogata, W., Certificateless Aggregate Signature Schemes with Improved Security. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* e98.a(1):92–99, 2015.
24. Chao, H. C., Chu, Y. M., and Lin, M. T., The implication of the next-generation wireless network design: cellular mobile IPv6. *IEEE Trans. Consum. Electron.* 46(3):656–663, 2000.
25. Goldwasser, S., Micali, S., and Rivest, R. L., A digital signature scheme secure against adaptive chosen-message attacks. *Siam Journal on Computing* 17(2):281–308, 1988.
26. Xing, D., Cao, Z., and Dong, X., Identity based signature scheme based on cubic residues. *SCIENCE CHINA Inf. Sci.* 54(10):2001–2012, 2011.